***In the Claims***

The status of claims in the case is as follows:

1. [Currently amended] A system for a web based trust model governing delivery of services and programs from a workflow, enterprise and mail-enabled application server and platform, comprising:

a connection protocol connecting a user client to a server site;

download utilities responsive to said connection protocol for downloading said services and programs from said server site to separate and non-conflicting execution spaces at said user client; and

trust assignment user interface dialogs responsive to said connection protocol for advising said user of risks taken when accepting executable download from said server site; and

said server site responsive to said user accepting said server site as trusted for centrally administering

security policies for said services and programs.

2. [Original] The system of claim 1, said connection protocol selectively being HTTP or HTTPS.

3. [Original] The system of claim 1, further comprising:

a processor for establishing security context, said processor including

a stage 1 processor for determining from said user if said server site is to be trusted; and

a stage 2 processor for establishing whether or not the identity of said web site is confirmed and determining from said user if processing should continue to include installation of programs on said client.

4. [Original] The system of claim 3, further comprising:

a client download page;

a download control element in said download page;

said processor being activated upon activation of said download control element within said download page initiating a download process first to establish a security context and then to download program executable files.

5. [Original] The system of claim 2, further comprising:

said download utilities being responsive to an SSL connection to said server for activating said dialog to advise said user that said server site has been verified as being what it represents itself to be and to query said user whether code is to be downloaded from said server site to said client.

6. [Original] The system of claim 5, said code being custom code.

7. [Currently amended] The system of claim 5, said download utilities being responsive to a connection from said client to said server being other than SSL for activating said dialog to advise said user that said server site has not been verified as being what it represents itself to be and to query ~~said~~ said user

whether code is to be downloaded from said server site to said client.

8. [Original] The system of claim 7, said code being custom code.

9. [Original] The system of claim 1, further comprising:

said download utilities being responsive to user acceptance of download from said server site of executable code for downloading said executable code to said client;

a trace utility for identifying originators of downloaded code.

10. [Original] The system of claim 9, said trace utility selectively identifying originators of signed agents through electronic signature, of custom code traceable to code vendor through web site relationship, or custom code directly created by said web site.

11. [Original] The system of claim 1, further comprising:

a first trust model for establishing level of traceable accountability for a subscription at download time over a secure connection protocol;

a second trust model for establishing a reduced level of traceable accountability, with traceable accountability established only for electronically signed agents used by said subscription over a connection protocol not verified as secure; and

said dialogs being responsive to said trust models.

12. [Currently amended] A method for governing delivery of services and programs from a workflow, enterprise and mail-enabled application server and platform according to a web based trust model, comprising the steps of:

establishing a connection protocol between a client and a web site;

responsive to said connection protocol, determining a trust level assignable to said web site relative to risks taken when accepting executable download from said web site;

advising a user at said client of said trust level assignable with respect to said risks to said web site; and

responsive to user acceptance of said risks and accepting said server site as trusted, downloading said services and programs from a server site to separate and non-conflicting execution spaces at said user client and centrally administering security policies for said services and programs.

13. [Original] The method of claim 12, further comprising the steps of:

displaying a download control element in a client download page;

responsive to user selection of said download control element or upon schedule, initiating a download process first to establish a security context and then to download program executable files from said server.

14. [Original] The method of claim 12, further comprising

the step of:

responsive to user acceptance of download from said server site of executable code, downloading said executable code to said client.

15. [Original] The method of claim 14, further comprising the step of:

identifying originators of downloaded code.

16. [Original] The method of claim 15, further comprising the step of

selectively identifying originators of signed agents through electronic signature, of custom code traceable to code vendor through web site relationship, or custom code directly created by said web site.

17. [Currently amended] The method of claim 12, further comprising the ~~seps~~ steps of

establishing a first trust model specifying a level of traceable accountability for a subscription at download

time over a secure connection protocol;

establishing a second trust model for specifying a reduced level of traceable accountability, with traceable accountability established only for electronically signed agents used by said subscription over a connection protocol not verified as secure; and

said dialogs being responsive to said trust models.

18. [Currently amended] A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for governing delivery of services and programs from a workflow, enterprise and mail-enabled application server and platform according to a web based trust model, said method steps comprising:

establishing a connection protocol between a client and a web site;

responsive to said connection protocol, determining a trust level assignable to said web site relative to risks taken when accepting executable download from

said web site;

advising a user at said client of said trust level assignable with respect to said risks to said web site; and

responsive to user acceptance of said risks and accepting said server site as trusted, downloading said services and programs from a server site to separate and non-conflicting execution spaces at said user client and centrally administering security policies for said services and programs.

19. [Currently amended] A computer program product configured to be operable to govern delivery of services and programs from a workflow, enterprise and mail-enabled application server and platform according to a web based trust model, according to the steps of:

establishing a connection protocol between a client and a web site;

responsive to said connection protocol, determining a trust level assignable to said web site relative to

risks taken when accepting executable download from said web site;

advising a user at said client of said trust level assignable with respect to said risks to said web site; and

responsive to user acceptance of said risks and accepting said server site as trusted, downloading said services and programs from a server site to separate and non-conflicting execution spaces at said user client and centrally administering security policies for said services and programs.